iBAQS-FX リリースノート

この度は、iBAQS-FX をお買い上げいただき、誠にありがとうございました。
このリリースノートは、バージョンアップにより追加される機能、仕様変更、修正内容をお知らせするものです。

ソフトウェアバージョン　4.0.0

ソフトウェアバージョン 3.0.0 未満からバージョンアップを行う場合には管理画面のアップデート完了画面で再起動をクリックしてからおよそ 20 分の間、管理画面へのアクセス、認証、IP アドレスの払い出し等の処理が行えない状態となります。管理画面へ再びアクセスできるようになる前に強制的に電源をお切りいただきますと正常に起動できない状態となりますのでご注意ください。
ダウンロードサイズが大きく、ご利用のネットワーク環境によってはアップデート処理完了時にセッションタイムアウトが発生する可能性があります。アップデート適用前にサーバ設定画面からセッションタイマーを長めに変更してください。アップデート完了時にセッションタイムアウトが発生してしまった場合には必ず再度ログインいただき、サーバ設定から再起動を手動で行ってください。
一度バージョンアップを行うとバージョンダウンを行うことができませんのでご注意ください。

1 新機能

ソフトウェアバージョン 3.1.3 から 4.0.0 へのバージョンアップにおいて、以下の機能が追加されました。

1.1　メーカー名表示を追加しました。
MAC 収集状況画面と不正アクセス状況画面において、検出した端末の MAC アドレスに対するメーカー名の表示を追加しました。

1.2　各種エクスポート機能を追加しました。
MAC 収集状況情報、不正アクセス情報、クライアント状態のエクスポートが可能になりました。MAC 収集状況画面、不正アクセス状況画面、クライアント状態画面で利用可能です。

1.3　UPS 共有機能を追加しました。
1 台の UPS で 2 台の冗長構成の iBAQS-FX を共有することが可能になりました。
冗長構成時のプライマリ機の「UPS 連携設定」画面から「冗長化時の共有」を「する」に選択することで設定が可能となります。UPS への給電が停止した場合、セカンダリ機からシャットダウンし、次にプライマリ機をシャットダウンします。復電した場合には、自動起動して通常運転となります。

1.4　リモート接続認証機能を追加しました。
スマートフォンからリモート接続認証が可能になりました。
スマートフォンからL2TPを利用してルータに接続し、ルータからiBAQS-FXに認証要求を投げ、認証結果に応じて、ネットワーク接続可否をコントロールすることができるようになりました。iBAQS-FX には認証スイッチとしてルータをネットワーク機器登録し、クライアントとしてユーザーID 認証に必要なユーザーID とパスワードを登録する必要があります。L2TP を利用した接続の詳細に関しては、スマートフォンおよびルータの取扱説明書をご参照ください。

1.5　対応ネットワーク機器に x200 スイッチを追加しました。

アライドテレシス社製 AT-x200 シリーズのスイッチをサポートしました。

1.6 冗長化自動再構成機能を追加しました。
冗長構成時のサーバの起動順に関わらず、常に「通常運転」となるようにすることが可能になりました。データの新しい方をプライマリ機と判断します。冗長化設定画面の再構成方式を「自動」にすることで可能となります。また、「手動」に設定することにより、今まで通りの動作も可能です。

1.7 集中管理機能を追加しました。
最大 100 台の iBAQS-FX を子機として登録し、親機から通信状況や不正アクセス件数、サービス状態などを一覧で確認することができ、子機の管理画面にワンクリックでアクセスできます。

1.8 事前登録承認機能を追加しました。
利用者自らが事前登録画面で登録を行い、管理者が承認を許可することでクライアント情報に登録されることが可能になりました。

1.9 対応 UPS に UPS-RS シリーズを追加しました。
APC 社製 UPS-RS シリーズをサポートしました。

1.10 Windows ドメイン認証機能を追加しました。
Windows NT4 ドメインサーバおよび Active Directory ドメインサーバを対象として、Windows ドメイン認証を行うことが可能になりました。認証方式として PEAP をサポートし、Windows ドメイン認証を行う場合、認証モードと併用して動作します。

1.11 証明書個別発行機能を追加しました。
利用者自らが認証局証明書のダウンロード、クライアント証明書の発行／失効／ダウンロードを行うことが可能になりました。管理画面のログインにて、クライアントを登録する際に設定したクライアント証明書のユーザーIDとパスワードを入力し、「証明書のお手続き」画面に遷移し、必要な操作を行います。

2 改善事項

ソフトウェアバージョン 3.1.3 から 4.0.0 へのバージョンアップにおいて、以下の項目が修正されました。

2.1 一定期間認証がないクライアントが存在する場合にアラート通知を行う機能において、最大 999 日まで一定期間認証なし日数を設定可能とするよう修正しました。

2.2 SNMP で OID:.1.3.6.1.2.1.1.2(sysObjectID)に応答できるよう修正し、MIB ファイルに載っていない OID に応答する問題を修正しました。

2.3 管理画面で選択された画面のメニュー項目をハイライト表示させるよう修正しました。

2.4 クライアント状態画面において、最終認証日時で検索できるよう修正しました。

2.5 検知モードで未登録クライアントから認証を受けた場合、管理ログに出力されない問題を修正しました。

2.6 入力フィールド項目の高さを入力しやすい高さに修正しました。

2.7 クライアント状態監視処理において、警告対象のクライアントが存在した場合、2 回目以降管理ログに出力されない問題を修正しました。

2.8 DHCP の再起動のタイミングで冗長化のリソースチェックを行うと、DHCP が停止してしまう問題を修正しました。

2.9 ピア IP アドレスに 1.1.1.1 を指定して冗長化設定を行った場合、失敗してしまう問題を修正しました。

2.10 MAC 収集モード（DHCP 無効）から自動登録を行う際、利用者名・PC 名が重複していても登録できてしまう問題を修正しました。

2.11 DHCP 無効時にサーバの IP アドレスが変更できない問題を修正しました。
2.12 冗長化設定での接続確認用の機器が停止している場合、フェールオーバーが起きてしまう問題を修正しました。
2.13 冗長構成を行っている場合、DHCP ログが出力されない問題を修正しました。
2.14 eth1 に設定した IP アドレスを eth0 側のネットワークに arp 告知してしまう問題を修正しました。
2.15 認証ログ画面で検索文字列を入力して検索した場合に正常に検索結果が得られない問題を修正しました。
2.16 セカンダリ機でオフラインライセンス設定を行った場合、システムエラーが表示される問題を修正しました。
2.17 ユーザーID 認証を行った場合、認証ログの PC 名に異なる PC 名が表示されてしまう場合がある問題を修正しました。
2.18 サーバ設定画面で入力チェックエラーとなった場合、基本タブに戻ってしまう問題を修正しました。
2.19 管理者メールアドレス未設定で、アラートメールを選択してもエラーとならない問題を修正しました。
2.20 管理者 ID とパスワードが認証用のユーザーID とパスワードとして登録できてしまう問題を修正しました。
2.21 一部のプロキシサーバ(*Z-PROXY Server* V2)を利用してライセンスの有効期限の取得に失敗してしまう問題を修正しました。
2.22 冗長化設定確認画面から戻るボタンをクリックすると、ローディング表示されてしまう問題を修正しました。
2.23 クライアント CSV 一括変更にて、MAC アドレス未設定で重複チェックエラーとなってしまう問題を修正しました。
2.24 バックアップファイル名にスペースが含まれているとリストアに失敗してしまう問題を修正しました。

3 制限事項

ソフトウェアバージョン 4.0.0 では以下の制限事項があります。

3.1 PEAP、EAP-TTLS 使用において内部認証に EAP 方式の認証を利用することが出来ません。
サポートする内部認証は下記の通りです。
・PEAP ： MS-CHAP v2　　・EAP-TTLS ： PAP
3.2 EAP-TTLS を利用する場合、外部認証のユーザーID は anonymous か内部認証と同一のユーザーID でなくてはなりません。anonymous を使用されることを推奨します。
3.3 外部認証局発行の証明書を使用して PEAP、EAP-TTLS、EAP-TLS 認証を行うことが出来ません。

4 注意事項

ソフトウェアバージョン 4.0.0 では以下の注意事項があります。

4.1 バージョン 3.X 以前のクライアントの「認証対象」が、バージョン 4.0 からは「認証パターン」という表現となったことを受け、次のように移行されます。

アップデート前の「認証対象」	アップデート後の「認証パターン」
「ユーザーID」と「クライアント証明書」にチェック	「クライアント証明書　認証」を選択
「MAC アドレス」、「ユーザーID」、「クライアント証明書」のすべてにチェック	「MAC アドレス認証」を選択

表示上は上記のように表示されますが、認証データは変更せずに移行するため、認証ができなくなることはありません。

以上